Use Well-Known Cryptography Appropriately and Correctly

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03 L4 / D/P[4]

Failing to use, or inventing your own, cryptography can introduce vulnerability.

Description

The following are frequent misuses of cryptography:

- Poor source of random numbers for a cryptographic algorithm.
- Not managing key material safely.
- Attempting to hide cryptographic credentials in client software or on client systems.
- Use of homegrown cryptographic algorithms.
- Use of homegrown implementation of well-known cryptographic algorithms.

References

[Anderson 93] Ross Anderson. *Why Cryptosystems Fail*. http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/wcf.pdf (1993).

[McArdle 01] Lorah McArdle. *Beyond Encryption*. http://www.sdmagazine.com/documents/s=818/sdm0101i/ (2001).

[Menezes 96] Menezes, Alfred J.; Van Oorschot, Paul C.; & Vanstone, Scott A. *Handbook of Applied Cryptography*. CRC Press, 1996.

[Morar 00] Morar, John F. & Chess, David M. *Can Cryptography Prevent Computer Viruses?* http://www.research.ibm.com/antivirus/SciPapers/VB2000JFM.htm (2000).

[Schneier 96] Schneier, Bruce. *Why Cryptography Is Harder Than It Looks*. http://www.schneier.com/essay-037.pdf (1996).

[Schneier 98] Schneier, Bruce. "Cryptographic Design Vulnerabilities." *Computer 31*, 9 (1998): 29-33.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[3] file:///portal/vitae/william_l_fithen

[1] mailto:permission@sei.cmu.edu

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.